Network Working Group
Request for Comments: 1173

J. Van Bokkelen
FTP Software, Inc.
August 1990

Responsibilities of Host and Network Managers
A Summary of the "Oral Tradition" of the Internet

Status of this Memo

This informational RFC describes the conventions to be followed by those in charge of networks and hosts in the Internet. It is a summary of the "oral tradition" of the Internet on this subject. [RFC Editor's note: This memo is a contribution by the author of his view of these conventions. It is expected that this RFC will provide a basis for the development of official policies in the future.] These conventions may be supplemented or amended by the policies of specific local and regional components of the Internet. This RFC does not specify a standard, or a policy of the IAB. Distribution of this memo is unlimited.

Table of Contents

Status of this Memo 1
1. Basic Responsibilities..... 1
2. Responsibilities of Network Managers..... 2
3. Responsibilities of Host System Managers..... 2
4. Postmaster@foo.bar.baz..... 3
5. Problems and Resolutions..... 3
6. The Illusion of Security..... 4
7. Summary..... 5
8. Security Considerations..... 5
9. Author's Address..... 5

1. Basic Responsibilities

The Internet is a co-operative endeavor, and its usefulness depends on reasonable behaviour from every user, host and router in the Internet. It follows that people in charge of the components of the Internet MUST be aware of their responsibilities and attentive to local conditions. Furthermore, they MUST be accessible via both Internet mail and telephone, and responsive to problem reports and diagnostic initiatives from other participants.

Even local problems as simple and transient as system crashes or power failures may have widespread effects elsewhere in the net. Problems which require co-operation between two or more responsible individuals to diagnose and correct are relatively common. Likewise,

the tools, access and experience needed for efficient analysis may not all exist at a single site.

This communal approach to Internet management and maintenance is dictated by the present decentralized organizational structure. The structure, in turn, exists because it is inexpensive and responsive to diverse local needs. Furthermore, for the near term, it is our only choice; I don't see any prospect of either the government or private enterprise building a monolithic, centralized, ubiquitous "Ma Datagram" network provider in this century.

2. Responsibilities of Network Managers

One or more individuals are responsible for every IP net or subnet which is connected to the Internet. Their names, phone numbers and postal addresses MUST be supplied to the Internet NIC (or to the local or regional transit network's NIC) prior to the network's initial connection to the Internet, and updates and corrections MUST be provided in a timely manner for as long as the net remains connected.

In order to adequately deal with problems that may arise, a network manager must have either:

A. System management access privileges on every host and router connected to the local network, or:

B. The authority and access to either power off, re-boot, physically disconnect or disable forwarding IP datagrams from any individual host system that may be misbehaving.

For all networks, a network manager capable of exercising this level of control MUST be accessible via telephone 8 hours a day, 5 days a week. For nets carrying transit traffic, a network manager SHOULD be accessible via telephone 24 hours a day.

3. Responsibilities of Host System Managers

One or more individuals must be responsible for every host connected to the Internet. This person MUST have the authority, access and tools necessary to configure, operate and control access to the system. For important timesharing hosts, primary domain name servers and mail relays or gateways, responsible individual(s) SHOULD be accessible via telephone 24 hours a day, 7 days a week.

For less-important timesharing hosts or single-user PCs or workstations, the responsible individual(s) MUST be prepared for the possiblity that their network manager may have to intervene in their

absence, should the resolution of an Internet problem require it.

4. Postmaster@foo.bar.baz

Every Internet host that handles mail beyond the local network MUST maintain a mailbox named "postmaster". In general, this should not simply forward mail elsewhere, but instead be read by a system maintainer logged in to the machine. This mailbox SHOULD be read at least 5 days a week, and arrangements MUST be made to handle incoming mail in the event of the absence of the normal maintainer.

A machine's "postmaster" is the normal point of contact for problems related to mail delivery. Because most traffic on the long-haul segments of the Internet is in the form of mail messages, a local problem can have significant effects elsewhere in the Internet. Some problems may be system-wide, such as disk or file system full, or mailer or domain name server hung, crashed or confused. Others may be specific to a particular user or mailing list (incorrect aliasing or forwarding, quota exceeded, etc.).

In either case, the maintainer of a remote machine will normally send mail about delivery problems to "postmaster". Also, "postmaster" is normally specified in the "reply-to:" field of automatically generated mail error messages (unable to deliver due to nonexistent user name, unable to forward, malformed header, etc.). If this mailbox isn't read in a timely manner, significant quantities of mail may be lost or returned to its senders.

5. Problems and Resolutions

Advances in network management tools may eventually make it possible for a network maintainer to detect and address most problems before they affect users, but for the present, day-to-day users of networking services represent the front line. No responsible individual should allow their "dumb-question" filter to become too restrictive; reports of the form "I haven't gotten any mumblefrotz mail for a week... " or "I could get there this morning, but not now..." should always get timely attention.

There are three basic classes of problems that may have network-wide scope: User-related, host-related and network-related.

A. User-related problems can range from bouncing mail or uncivilized behaviour on mailing lists to more serious issues like violation of privacy, break-in attempts or vandalism.

B. Host-related problems may include mis-configured software,

obsolete or buggy software and security holes.

C. Network-related problems are most frequently related to routing: incorrect connectivity advertisements, routing loops and black holes can all have major impacts. Mechanisms are usually in place for handling failure of routers or links, but problems short of outright failure can also have severe effects.

Each class of problem has its own characteristics. User-related problems can usually be solved by education, but system managers should be aware of applicable federal and state law as well; Privacy violations or "cracking" attempts have always been grounds for pulling a user's account, but now they can also result in prosecution. Host-related problems are usually resolvable by re-configuration or upgrading the software, but sometimes the manufacturer needs to be made aware of a bug, or jawboned into doing something about it; Bugs that can't be fixed may be serious enough to require partial or total denial of service to the offending system. Similar levels of escalation exist for network-related problems, with the solution of last resort being ostracism of the offending net.

6. The Illusion of Security

Every host and network manager MUST be aware that the Internet as presently constituted is NOT secure. At the protocol level, much more effort has been put into interoperability, reliability and convenience than has been devoted to security, although this is changing. Recent events have made software developers and vendors more sensitive to security, in both configuration and the underlying implementation, but it remains to be demonstrated how much long-term effect this will have. Meanwhile, the existing system survives through the co-operation of all responsible individuals.

Security is subjective; one site might view as idle curiosity what another would see as a hostile probe. Since ultimately the existence of the Internet depends on its usefulness to all members of the community, it is important for managers to be willing to accept and act on other sites' security issues, warning or denying access to offending users. The offended site, in turn, must be reasonable in its demands (someone who set off an alarm while idly seeing if the sendmail "DEBUG" hole was closed on a "sensitive" host probably should be warned, rather than prosecuted).

Because Internet security issues may require that local management people either get in touch with any of their users, or deny an offending individual or group access to other sites, it is necessary that mechanisms exist to allow this. Accordingly, Internet sites

SHOULD NOT have "general use" accounts, or "open" (without password) terminal servers that can access the rest of the Internet.

In turn, the "sensitive" sites MUST be aware that it is impossible in the long term to deny Internet access to crackers, disgruntled former employees, unscrupulous competitors or agents of other countries. Getting an offender flushed is at best a stop-gap, providing a breathing space of a day or an hour while the security holes under attack are closed. It follows that each host's manager is ultimately responsible for its security; the more "sensitive" the application or data, the more intimate the manager must be with the host's operating system and network software and their foibles.

7. Summary

The heart of the Internet is the unique community of interest encompassing its users, operators, maintainers and suppliers. Awareness and acceptance of the shared interest in a usable Internet is vital to its survival and growth. The simple conventions presented here should be supplemented by common sense as necessary to achieve that end.

8. Security Considerations

Security issues are discussed in Sections 5 and 6.

9. Author's Address

James B. VanBokkelen
FTP Software Inc.
26 Princess St.
Wakefield, MA 01880

Phone: 617-246-0900

EMail: jbvb@ftp.com